

**RECEIVED
CENTRAL FAX CENTER**

APR 30 2007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Francisco Corella Examiner: Christopher J. Brown
Serial No.: 09/483,185 Group Art Unit: 2134
Filed: January 14, 2000 Docket No.: 10991054-1
Title: AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY

CERTIFICATE OF TRANSMISSION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

I hereby certify that the following paper(s) are being facsimile transmitted to the U.S. Patent and Trademark Office, Fax. No. (571) 273-8300 on the date shown below:

Transmittal of Appeal Brief (1 pg.); and
Appeal Brief under 37 C.F.R. 41.37 (19 pgs.).

Date: 4-30-07
PGB: hsf

By: 
Name: Patrick G. Billig (Reg. No. 38,080)

21 Pages (including cover page)

**RECEIVED
CENTRAL FAX CENTER**

APR 30 2007

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10991054-1IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Francisco Corella

Confirmation No.: 8069

Application No.: 09/483,185

Examiner: Christopher J. Brown

Filing Date: January 14, 2000

Group Art Unit: 2134

Title: AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450TRANSMITTAL OF APPEAL BRIEFTransmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on February 28, 2007.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) \$500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:☐ 1st Month
\$120☐ 2nd Month
\$450☐ 3rd Month
\$1020☐ 4th Month
\$1580☐ The extension fee has already been filed in this application.☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.Please charge to Deposit Account 08-2025 the sum of \$ 500. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.☐ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:
Commissioner for Patents, Alexandria, VA 22313-1450
Date of Deposit:

OR

☒ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.

Date of facsimile: April 30, 2007

Typed Name: Patrick G. Billig

Signature: 

Respectfully submitted,

Francisco Corella

By 

Patrick G. Billig

Attorney/Agent for Applicant(s)

Reg No.: 38,060

Date: April 30, 2007

Telephone: (612) 573-2003

003
RECEIVED
CENTRAL FAX CENTER

APR 30 2007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicant:	Francisco Corella	Examiner:	Christopher J. Brown
Serial No.:	09/483,185	Group Art Unit:	2134
Filed:	January 14, 2000	Docket No.:	10991054-1
Title:	AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY		

APPEAL BRIEF UNDER 37 C.F.R. §41.37

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir/Madam:

This Appeal Brief is submitted in support of the Notice of Appeal filed on February 28, 2007, appealing the final rejection of claims 1, 3, 4, 6-13, 15, 16 and 18-24 of the above-identified application as set forth in the Final Office Action mailed November 28, 2006.

The U.S. Patent and Trademark Office is hereby authorized to charge Deposit Account No. 08-2025 in the amount of \$500.00 for filing a Brief in Support of an Appeal as set forth under 37 C.F.R. §41.20(b)(2). At any time during the pendency of this application, please charge any required fees or credit any overpayment to Deposit Account No. 08-2025.

Appellant respectfully requests consideration and reversal of the Examiner's rejection of pending claims 1, 3, 4, 6-13, 15, 16 and 18-24.

05/02/2007 CCHAU1 00000070 082025 09483185

01 FC:1402 500.00 DA

Appeal Brief to the Board of Patent Appeals and Interferences

Applicant: Francisco Corella

Serial No.: 09/483,185

Filed: January 14, 2000

Docket No.: 10991054-1

Title: AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY**TABLE OF CONTENTS**

Real Party in Interest	3
Related Appeals and Interferences	3
Status of Claims.....	3
Status of Amendments.....	3
Summary of The Claimed Subject Matter.....	3
Grounds of Rejection to be Reviewed on Appeal	5
Argument.....	5
Conclusion	13
Claims Appendix	14
Evidence Appendix.....	18
Related Proceedings Appendix.....	19

Appeal Brief to the Board of Patent Appeals and Interferences

Applicant: Francisco Corella

Serial No.: 09/483,185

Filed: January 14, 2000

Docket No.: 10991054-1

Title: AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY**REAL PARTY IN INTEREST**

The real party in interest is Hewlett-Packard Development Company, LP having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellant that will have a bearing on the Board's decision in the present Appeal.

STATUS OF CLAIMS

In a Final Office Action mailed November 28, 2006, claims 1, 3, 4, 6-13, 15, 16, and 18-24 were finally rejected. Claims 1, 3, 4, 6-13, 15, 16, and 18-24 are pending in the application, and are the subject of the present Appeal.

STATUS OF AMENDMENTS

No amendments have been entered subsequent to the Final Office Action mailed November 28, 2006. The claims listed in the Claims Appendix, therefore, reflect the claims as of November 28, 2006.

SUMMARY OF THE CLAIMED SUBJECT MATTER

The Summary is set forth as exemplary embodiments corresponding to the language of independent claims 1 and 13. Discussions about elements of claims 1 and 13 can be found at least at the cited locations in the specification and drawings.

One aspect of the present invention, as claimed in independent claim 1, provides a public key authorization infrastructure (30) comprising a client program (34) accessible by a user and an application program (36, 38, 40). The public key authorization infrastructure comprises a certificate authority (32) issuing a long-term public key identity certificate (long-term certificate) (60) that binds a public key (64) of the user to long-term identification

Appeal Brief to the Board of Patent Appeals and Interferences

Applicant: Francisco Corella

Serial No.: 09/483,185

Filed: January 14, 2000

Docket No.: 10991054-I

Title: AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY

information (66) related to the user. The public key authorization infrastructure comprises a directory (42) for storing short-term authorization information related to the user. The public key authorization infrastructure comprises a credentials server (44) for issuing a short-term public key credential certificate (short-term certificate) (70) to the client, the short-term certificate binds the public key of the user to the long-term identification information related to the user from the long term certificate and to the short-term authorization information (77) related to the user from the directory. The short-term certificate includes meta-data (72) related to the short-term certificate and at least one of an expiration date and an expiration time and is never subject to revocation. The client program presents the short-term certificate to the application program for authorization and demonstrates that the user has knowledge of a private key (46) corresponding to the public key in the short-term certificate. *See specification at page 9, line 11 through page 14, line 30; and Figures 1-4.*

One aspect of the present invention, as claimed in independent claim 13, provides a method of authorizing a user comprising issuing a long-term public key identity certificate (long-term certificate) (60) that binds a public key (64) of the user to long-term identification information (66) related to the user. The method comprises storing short-term authorization information (77) related to the user. The method comprises issuing a short-term public key credential certificate (short-term certificate) (70) that binds the public key of the user to the long-term identification information related to the user contained in the long-term certificate and to the short-term authorization information related to the user wherein the short-term certificate includes meta-data (72) related to the short-term certificate and at least one of an expiration date and an expiration time and is never subject to revocation. The method includes presenting the short-term certificate on behalf of the user to an application program for authorization and demonstrating that the user has knowledge of a private key (46) corresponding to the public key in the short-term certificate. *See specification at page 15, line 1 through page 16, line 16; and Figure 5 for an embodiment of a generalized authorization protocol. See specification at page 16, line 17 through page 24, line 26; and Figures 6-9 for an embodiment of amore detailed authorization protocol. See also specification at page 9, line 11 through page 14, line 30; and Figures 1-4 for the describing and illustrating an embodiment of a public key authorization infrastructure that can perform the method of independent claim 13.*

Appeal Brief to the Board of Patent Appeals and Interferences

Applicant: Francisco Corella

Serial No.: 09/483,185

Filed: January 14, 2000

Docket No.: 10991054-1

Title: AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY**GROUND OF REJECTION TO BE REVIEWED ON APPEAL**

- I. Claims 1, 3, 6, 8, 10, 13, 15, 18, 20 and 22 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Riggins US Patent No. 6,233,341 in view of Butt US Patent No. 6,754,829.
- II. Claim 4 and 16 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Riggins US Patent No. 6,233,341 in view of Butt US Patent No. 6,754,829 in view of Noar US Patent No. 6,226,743.
- III. Claims 7, 9, 19 and 21 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Riggins US Patent No. 6,233,341 in view of Butt US Patent No. 6,754,829 in view of Howell US Patent No. 5,276,901.
- IV. Claims 11 and 23 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Riggins US Patent No. 6,233,341 in view of Butt US Patent No. 6,754,829 in view of Maruyama US Patent No. 6,393,563.
- V. Claims 12 and 24 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Riggins US Patent No. 6,233,341 in view of Butt US Patent No. 6,754,829 in view of Kausik US Patent No. 6,263,446.

ARGUMENT**I. The Applicable Law**

With regard to a 35 U.S.C. § 103 obviousness rejection: "Patent examiners carry the responsibility of making sure that the standard of patentability enunciated by the Supreme Court and by the Congress is applied in each and every case." M.P.E.P. 2141 (emphasis in the original). The Examiner bears the burden under 35 U.S.C. § 103 in establishing a *prima facie* case of obviousness. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988).

Three criteria must be satisfied to establish a *prima facie* case of obviousness. First, the Examiner must show that some objective teaching in the prior art or some knowledge generally available to one of ordinary skill in the art would teach, suggest, or motivate one to modify a reference or to combine the teachings of multiple references. *In re Fine* at 1074. Second, the prior art can be modified or combined only so long as there is a reasonable

Appeal Brief to the Board of Patent Appeals and Interferences

Applicant: Francisco Corella

Serial No.: 09/483,185

Filed: January 14, 2000

Docket No.: 10991054-1

Title: AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY

expectation of success. *In re Merck & Co., Inc.*, 800 F.2d 1091, 231 USPQ 375, 379 (Fed. Cir. 1986). Third, the reference or combined references must teach or suggest all of the claim limitations. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (C.C.P.A. 1974).

The court in *Fine* stated:

Obviousness is tested by "what the combined teaching of the references would have suggested to those of ordinary skill in the art." But it "cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination." And "teachings of references can be combined *only* if there is some suggestion or incentive to do so."

In re Fine, 5 USPQ2d at 1599 (citations omitted).

There must be some teaching somewhere that provides the suggestion or motivation to combine prior art teachings and applies that combination to solve the same or similar problem that it addresses. *In re Nilssen*, 851 F.2d 1401, 1403, 7 USPQ2d 1500, 1502 (Fed. Cir. 1988); *In re Wood*, 599 F.2d 1032, 1037, 202 USPQ 171, 174 (C.C.P.A. 1979). In particular, "The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based upon Appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991); M.P.E.P. § 2142 (emphasis added).

The test for obviousness under § 103 must take into consideration the invention as a whole; that is, one must consider the particular problem solved by the combination of elements that define the invention. *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1143, 227 USPQ 543, 551 (Fed. Cir. 1985). Furthermore, claims must be interpreted in light of the specification, claim language, other claims, and prosecution history. *Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561, 1568, 1 USPQ2d 1593, 1597 (Fed. Cir. 1987), *cert. denied*, 481 U.S. 1052 (1987). At the same time, a prior patent cited as a § 103 reference must be considered in its entirety, "*i.e.* as a *whole*, including portions that lead away from the invention." *Id.* That is, the Examiner must recognize and consider not only the similarities, but also the critical differences between the claimed invention and the prior art as one of the factual inquiries pertinent to any obviousness inquiry under 35 U.S.C. § 103. *In re Bond*, 910 F.2d 831, 834, 15 USPQ2d 1566, 1568 (Fed. Cir. 1990) (emphasis added). Finally, the Examiner must avoid hindsight. *Id.*

Appeal Brief to the Board of Patent Appeals and Interferences

Applicant: Francisco Corella

Serial No.: 09/483,185

Filed: January 14, 2000

Docket No.: 10991054-1

Title: AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY

With regard for the test for obviousness under § 103, a statement that modifications of the prior art to meet the claimed invention would have been “ ‘well within the ordinary skill of the art’ at the time the claimed invention was made ” because the references relied upon teach that all aspects of the claimed invention were individually known in the art is not sufficient to establish a *prima facie* case of obviousness without some objective reason to combine the teachings of the references. *Ex parte Levengood*, 28 USPQ2d 1300 (Bd. Pat. App. & Inter. 1993); M.P.E.P. § 2143.01 (emphasis in the original).

In conclusion, an Appellant is entitled to a patent grant if any one of the elements of a *prima facie* case of obviousness is not established. The Federal Circuit has endorsed this view in stating: “If examination at the initial stage does not produce a *prima facie* case of unpatentability, then without more the Appellant is entitled to grant of the patent.” In *re Oetiker*, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1448 (Fed. Cir. 1992).

II. Rejection of claims 1, 3, 6, 8, 10, 13, 15, 18, 20 and 22 under 35 U.S.C. §103(a) as being unpatentable over Riggins US Patent No. 6,233,341 in view of Butt US Patent No. 6,754,829.

The Examiner admits that the Riggins patent does not teach a short-term certificate that is not subject to revocation prior to expiration. Thus, the Riggins patent does not teach or suggest the limitations of amended independent claims 1 and 13 that the short-term certificate “is never subject to revocation.” The Examiner cites that Butt et al. patent to teach short lived certificates that removes the need for revocation.

The combination of the Riggins patent and the Butt et al. patent, however, does not teach or suggest the limitations of amended independent claims 1 and 13 of the short-term certificate including at least one of an expiration date and an expiration time and is never subject to revocation. The Riggins patent at column 3, lines 17-19 states that “[t]emporary certificates can safely be installed because they expire quickly and can be revoked when the user leaves the remote site.” The Riggins patent illustrates a client method for managing a temporary certificate 400 in Figure 8 and states at column 13, lines 40-47 that

If the certificate maintenance Downloadable has determined that the temporary certificate 400 has almost expired, the certificate maintenance downloadable 340 in step 825 determines whether the user is done with the session, preferably, by asking the user. If the

Appeal Brief to the Board of Patent Appeals and Interferences

Applicant: Francisco Corella

Serial No.: 09/483,185

Filed: January 14, 2000

Docket No.: 10991054-1

Title: **AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY**

user is done, then the certificate maintenance Downloadable 345 in step 855 de-installs the temporary certificate 400.

The Riggins patent at column 14, lines 6-12 further states

If the temporary certificate 400 has not almost expired, then the certificate maintenance Downloadable in step 820 waits. The certificate maintenance Downloadable 340 in step 845 determines if the user is done with the session. If not, then the method 800 returns to step 815. Otherwise, the certificate maintenance Downloadable 340 in step 850 **adds the temporary certificate 400 to the revocation list 335.** (*emphasis added*)

The Riggins patent states at column 14, lines 46-48 "the secure communications engine 147 determines if the temporary certificate 400 has expired or whether the user has logged out." Thus, in the Riggins system that uses a temporary certificate at a remote site, the system relies on that when the user logs out of the remote site that the temporary certificate is revoked. Contrary to the Examiners assertion in the Final Office Action, in Figure 8 and the corresponding text of the Riggins patent, the temporary certificate will be revoked if the certificate is not almost expired and the user is done with the session (i.e. logged out), and in the method illustrated in Figure 9, the secure communication engine only needs to determine if the temporary certificate has expired or whether the user has logged out.

The Butt et al. patent discloses beginning at column 9, line 32 that the core only grants session certificates to authenticated operators, and session certificates are created on-the-fly, and then destroyed once an operator's session with the manageable device has terminated, and that once a console session terminates the certificate (and its private key) is automatically lost.

Thus, in the Riggins system that uses a temporary certificate at a remote site, the system relies on that when the user logs out of the remote site that the temporary certificate is revoked and in the Butt et al. patent the session certificate is destroyed and the certificate (and its private key) is automatically lost once the session terminates. By contrast, if a similar embodiment is implemented according to the invention claimed in amended independent claims 1 and 13, when a session terminates or when a user logs out of a remote site, as long as the at least one of an expiration date and an expiration time has not expired, the short-term certificate can still be used, because as recited in claims 1 and 13 the short term certificate is **never subject to revocation.**

Appeal Brief to the Board of Patent Appeals and Interferences

Applicant: Francisco Corella

Serial No.: 09/483,185

Filed: January 14, 2000

Docket No.: 10991054-1

Title: AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY

Furthermore, there is no teaching or suggestion to combine teaching of the Butt et al. patent with the Riggins patent to arrive at the invention claimed in amended independent claims 1 and 13. In fact, Riggins teaches away from a short-term certificate that is never subject to revocation as recited in amended independent claims 1 and 13. For example in the Abstract, the Riggins patent specifically states that "[t]he web server engine maintains a revocation list that contains information identifying revoked temporary certificates, so that a revoked but thus far unexpired certificate can not be improperly used. The web site reviews the temporary certificate for authenticity and contacts the global server site to review the revocation list and determine whether the temporary certificate has been revoked."

There is also no reasonable expectation of success for this suggested combination as stated in the Riggins patent at column 3, lines 17-19 "[t]emporary certificates can safely be installed because they expire quickly and can be revoked when the user leaves the remote site," and in Figure 8 and the corresponding text of the Riggins patent, the temporary certificate will be revoked if the certificate is not almost expired and the user is done with the session(i.e. logged out), and in the method illustrated in Figure 9, the secure communication engine determines if the temporary certificate has expired or whether the user has logged out. Thus, in the Riggins system that uses a temporary certificate at a remote site, the system relies on that when the user logs out of the remote site that the temporary certificate is revoked. Thus, there would be no reasonable expectation of success if such capabilities would be removed from the Riggins system.

Furthermore, the Examiner does not cite a reference for a directory for storing short-term authorization information related to the user as recited in amended independent claim 1. The Examiner states that the Riggins patent does not specifically disclose **short term authorization information related to a user**. Therefore, the Riggins patent does not teach or suggest a directory for storing **short-term authorization information related to the user**, as recited in amended independent claim 1. Moreover, the Riggins patent also does not teach a short-term certificate binding the public key of the user to long-term identification information related to the user from the long-term certificate and to **the short-term authorization information related to the user from the directory** as recited in amended independent claim 1.

Appeal Brief to the Board of Patent Appeals and Interferences

Applicant: Francisco Corella

Serial No.: 09/483,185

Filed: January 14, 2000

Docket No.: 10991054-1

Title: AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY

The Examiner cites the Butt et al. patent for teaching short-term authorization information related to the user. However, the Butt et al. patent discloses beginning at column 9, line 58 one embodiment having a field indicating unbound access privileges, which is inserted by the core/certificate authority if the core determines that a "super user" attribute should be inserted. Thus, field indicating unbound access privileges is not stored in a directory. Thus, the Butt et al. patent does not teach or suggest a **directory** for storing short-term authorization information related to the user, as recited in amended independent claim 1. Moreover, the Butt et al. patent also does not teach a short-term certificate binding the public key of the user to long-term identification information related to the user from the long-term certificate and to the short-term authorization information related to the user from the **directory** as recited in amended independent claim 1.

One advantage of an embodiment of the invention having the short-term authorization information stored in a directory is disclosed in the present specification at page 11 lines 1-5 which states:

In one embodiment, credentials server 44 obtains the short-term information data needed to issue the short-term certificates from LDAP directory 42. In this embodiment, since credentials server 44 does not contain this short-term information data, credentials server 44 is easily replicated within public key authorization infrastructure 30 for increased performance.

In view of the above, the combination of the Riggins patent, and the Butt et al. patent does not establish any of the three criteria of a *prima facie* case of obviousness toward amended independent claims 1 and 13.

Dependent claims 3, 6, 8, and 10 are allowable as depending from an allowable base claim (claim 1) and are allowable on further independent grounds in view of the novel and nonobvious features and combinations set forth therein. Dependent claims 15, 18, 20, and 22 are allowable as depending from an allowable base claim (claim 13) and are allowable on further independent grounds in view of the novel and nonobvious features and combinations set forth therein.

Therefore, Appellants respectfully request reversal of the rejection of claims 1, 3, 6, 8, 10, 13, 15, 18, 20, and 22 under 35 U.S.C. § 103 and request allowance of these claims.

Appeal Brief to the Board of Patent Appeals and Interferences

Applicant: Francisco Corella

Serial No.: 09/483,185

Filed: January 14, 2000

Docket No.: 10991054-1

Title: AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY

III. Rejection of claim 4 and 16 under 35 U.S.C. §103(a) as being unpatentable over Riggins US Patent No. 6,233,341 in view of Butt US Patent No. 6,754,829 in view of Noar US Patent No. 6,226,743.

Dependent claim 4 is allowable as depending from an allowable base claim (claim 1) and is allowable on further independent grounds in view of the novel and nonobvious features and combinations set for therein. Dependent claim 16 is allowable as depending from an allowable base claim (claim 13) and is allowable on further independent grounds in view of the novel and nonobvious features and combinations set forth therein.

Therefore, Appellants respectfully request reversal of the rejection of claims 4 and 16 under 35 U.S.C. § 103 and request allowance of these claims.

IV. Rejections of claims 7, 9, 19 and 21 under 35 U.S.C. §103(a) as being unpatentable over Riggins US Patent No. 6,233,341 in view of Butt US Patent No. 6,754,829 in view of Howell US Patent No. 5,276,901.

Dependent claims 7 and 9 are allowable as depending from an allowable base claim (claim 1) and are allowable on further independent grounds in view of the novel and nonobvious features and combinations set for therein. Dependent claims 19 and 21 are allowable as depending from an allowable base claim (claim 13) and are allowable on further independent grounds in view of the novel and nonobvious features and combinations set forth therein.

Therefore, Appellants respectfully request reversal of the rejection of claims 7, 9, 19, and 21 under 35 U.S.C. § 103 and request allowance of these claims.

V. Rejection of claims 11 and 23 under 35 U.S.C. §103(a) as being unpatentable over Riggins US Patent No. 6,233,341 in view of Butt US Patent No. 6,754,829 in view of Maruyama US Patent No. 6,393,563.

Dependent claim 11 is allowable as depending from an allowable base claim (claim 1) and is allowable on further independent grounds in view of the novel and nonobvious features and combinations set for therein. Dependent claim 23 is allowable as depending from an allowable base claim (claim 13) and is allowable on further independent grounds in view of the novel and nonobvious features and combinations set forth therein.

Appeal Brief to the Board of Patent Appeals and Interferences

Applicant: Francisco Corella

Serial No.: 09/483,185

Filed: January 14, 2000

Docket No.: 10991054-1

Title: AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY

Therefore, Appellants respectfully request reversal of the rejection of claims 11 and 23 under 35 U.S.C. § 103 and request allowance of these claims.

VI. Rejection of claims 12 and 24 under 35 U.S.C. §103(a) as being unpatentable over Riggins US Patent No. 6,233,341 in view of Butt US Patent No. 6,754,829 in view of Kausik US Patent No. 6,263,446.

Dependent claim 12 is allowable as depending from an allowable base claim (claim 1) and is allowable on further independent grounds in view of the novel and nonobvious features and combinations set for therein. Dependent claim 24 is allowable as depending from an allowable base claim (claim 13) and is allowable on further independent grounds in view of the novel and nonobvious features and combinations set forth therein.

Therefore, Appellants respectfully request reversal of the rejection of claims 12 and 24 under 35 U.S.C. § 103 and request allowance of these claims.

Appeal Brief to the Board of Patent Appeals and Interferences

Applicant: Francisco Corella

Serial No.: 09/483,185

Filed: January 14, 2000

Docket No.: 10991054-1

Title: AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY**CONCLUSION**

For the above reasons, Appellants respectfully submit that the cited references neither anticipate nor render obvious claims of the pending Application. The pending claims distinguish over the cited references, and therefore, Appellants respectfully submit that the rejections must be withdrawn, and respectfully request the Examiner be reversed and claims 1, 3, 4, 6-13, 15, 16, and 18-24 be allowed.

Any inquiry regarding this Response should be directed to either Patrick G. Billig at the below-listed telephone numbers or Kevin Hart at Telephone No. (970) 898-7057, Facsimile No. (970) 898-7247. In addition, all correspondence should continue to be directed to the following address:

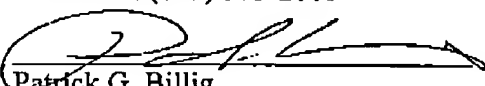
IP Administration
Legal Department, M/S 35
HEWLETT-PACKARD COMPANY
P.O. Box 272400
Fort Collins, Colorado 80527-2400

Respectfully submitted,

Francisco Corella

By his attorneys,

DICKE, BILLIG & CZAJA, PLLC
Fifth Street Towers, Suite 2250
100 South Fifth Street
Minneapolis, MN 55402
Telephone: (612) 573-2003
Facsimile: (612) 573-2005

Dated: 4-30-07
PGB:hsf
Patrick G. Billig
Reg. No. 38,080**CERTIFICATE UNDER 37 C.F.R. 1.8:**

The undersigned hereby certifies that this paper or papers, as described herein, are being transmitted via telefacsimile to Fax No. (571) 273-8300 on this 30 day of Apr, 2007.

By: 

Name: Patrick G. Billig

Appeal Brief to the Board of Patent Appeals and Interferences

Applicant: Francisco Corella

Serial No.: 09/483,185

Filed: January 14, 2000

Docket No.: 10991054-1

Title: AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY

CLAIMS APPENDIX

1. (Previously Presented) A public key authorization infrastructure comprising:
 - a client program accessible by a user;
 - an application program;
 - a certificate authority issuing a long-term public key identity certificate (long-term certificate) that binds a public key of the user to long-term identification information related to the user;
 - a directory for storing short-term authorization information related to the user; and
 - a credentials server for issuing a short-term public key credential certificate (short-term certificate) to the client, the short-term certificate binds the public key of the user to the long-term identification information related to the user from the long term certificate and to the short-term authorization information related to the user from the directory, wherein the short-term certificate includes meta-data related to the short-term certificate and at least one of an expiration date and an expiration time and is never subject to revocation, wherein the client program presents the short-term certificate to the application program for authorization and demonstrates that the user has knowledge of a private key corresponding to the public key in the short-term certificate.
2. (Cancelled)
3. (Previously Presented) The public key authorization infrastructure of claim 1 wherein a validity period from when the credentials server issues the short-term certificate to the at least one of expiration date and expiration time is sufficiently short such that the short-term certificate does not need to be subject to revocation.
4. (Previously Presented) The public key authorization infrastructure of claim 1 further comprising:
 - a certificate revocation list (CRL), wherein the at least one of expiration date and expiration time of the short-term certificate is before the CRL is next scheduled to be updated.

Appeal Brief to the Board of Patent Appeals and Interferences

Applicant: Francisco Corella

Serial No.: 09/483,185

Filed: January 14, 2000

Docket No.: 10991054-1

Title: AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY

5. (Cancelled)
6. (Original) The public key authorization infrastructure of claim 1 wherein the short-term certificate is a non-structured short-term certificate.
7. (Previously Presented) The public key authorization infrastructure of claim 1 further comprising:
a second application program; and
wherein the short-term certificate is a structured short-term certificate including:
a first folder corresponding to the first named application program and containing long-term information and short-term information as required by the first named application program;
a second folder corresponding to the second application program and containing long-term information and short-term information as required by the second application; and
wherein the first folder is open and the second folder is closed when the client presents the short-term certificate to the first named application program for authorization, wherein closing the second folder makes its contents not readable by the first named application program.
8. (Original) The public key authorization infrastructure of claim 1 wherein the short-term certificate is an X.509v3 certificate.
9. (Original) The public key authorization infrastructure of claim 7 wherein the first folder and the second folder are implemented as extension fields of an X.509v3 certificate.
10. (Original) The public key authorization infrastructure of claim 1 wherein the directory further stores the issued long-term certificate.
11. (Original) The public key authorization infrastructure of claim 1 wherein the private key is stored in a smartcard accessible by the client program.

Appeal Brief to the Board of Patent Appeals and Interferences

Applicant: Francisco Corella

Serial No.: 09/483,185

Filed: January 14, 2000

Docket No.: 10991054-1

Title: AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY

12. (Original) The public key authorization infrastructure of claim 1 wherein the private key is stored in a secure software wallet accessible by the client program.

13. (Previously Presented) A method of authorizing a user, the method comprising the steps of:

issuing a long-term public key identity certificate (long-term certificate) that binds a public key of the user to long-term identification information related to the user;

storing short-term authorization information related to the user;

issuing a short-term public key credential certificate (short-term certificate) that binds the public key of the user to the long-term identification information related to the user contained in the long-term certificate and to the short-term authorization information related to the user wherein the short-term certificate includes meta-data related to the short-term certificate and at least one of an expiration date and an expiration time and is never subject to revocation; and

presenting the short-term certificate on behalf of the user to an application program for authorization and demonstrating that the user has knowledge of a private key corresponding to the public key in the short-term certificate.

14. (Cancelled)

15. (Previously Presented) The method of claim 13 wherein a validity period from when the short-term certificate is issued to the at least one of expiration date and expiration time is sufficiently short such that the short-term certificate does not need to be subject to revocation.

16. (Previously Presented) The method of claim 13 further comprising the step of:

maintaining a certificate revocation list (CRL), wherein the at least one of expiration date and expiration time of the short-term certificate is before the CRL is next scheduled to be updated.

17. (Cancelled)

Appeal Brief to the Board of Patent Appeals and Interferences

Applicant: Francisco Corella

Serial No.: 09/483,185

Filed: January 14, 2000

Docket No.: 10991054-1

Title: AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY

18. (Original) The method of claim 13 wherein the short-term certificate is a non-structured short-term certificate.
19. (Previously Presented) The method of claim 13 wherein the short-term certificate is a structured short-term certificate including a first folder corresponding to the first named application program and containing long-term information and short-term information as required by the first named application program, and including a second folder corresponding to a second application program and containing long-term information and short-term information as required by the second application, wherein the method further comprises:
- closing the second folder and leaving the first folder open prior to the presenting step if the presenting step presents the short-term certificate to the first named application program for authorization, wherein closing the second folder makes its contents not readable by the first named application program.
20. (Original) The method of claim 13 wherein the short-term certificate is an X.509v3 certificate.
21. (Original) The method of claim 19 wherein the first folder and the second folder are implemented as extension fields of an X.509v3 certificate.
22. (Original) The method of claim 13 wherein the method further comprises the step of: storing the issued long-term certificate in a directory.
23. (Original) The method of claim 13 further comprising the step of: storing the private key in a smartcard.
24. (Original) The method of claim 13 further comprising the step of: storing the private key in a secure software wallet.

Appeal Brief to the Board of Patent Appeals and Interferences

Applicant: Francisco Corella

Serial No.: 09/483,185

Filed: January 14, 2000

Docket No.: 10991054-1

Title: AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY

EVIDENCE APPENDIX

None.

Appeal Brief to the Board of Patent Appeals and Interferences

Applicant: Francisco Corella

Serial No.: 09/483,185

Filed: January 14, 2000

Docket No.: 10991054-1

Title: AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY

RELATED PROCEEDINGS APPENDIX

None.